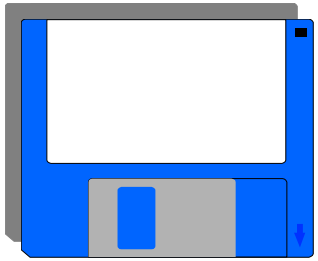
Security Channe

ne 1, Issue 2

Published by the
SA Security Education Community

2nd Quarte



AIS Security, Computer Forensics and the Insider Threat

Are You Really Safeguarding Classified Information?
A Frightening Look at the Insider Threat

It's 3am. The computer at work has been in as secure state for hours. The national security information processed by it safely protected -- or is it?

The other side of the world is waking to a new day. It's an atypically happy day for one foreign intelligence service (FIS) in particular. One of their agents has just handed over a disk containing U.S. national security information. How could this have happened? Did the FIS agent surreptitiously gain access to the classified AIS during the wee hours in the U.S. and download classified? No, nothing that elaborate. The FIS agent simply waited for the trusted employee to circumvent security.

Computer Crime, Computer Ethics and the Trusted Employee

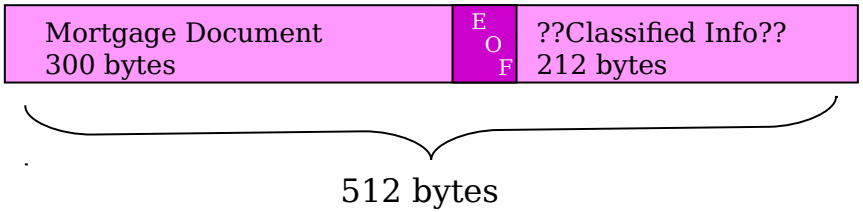
Several weeks earlier, a "trusted" employee used a classified computer to do some personal business. Baseball games, kids activities, etc. prevented the trusted employee from writing a letter to his mortgage company at home. He

The employee felt he was "honest." He brought the disk in from home, used his lunch hour to write the letter (on a classified system) and didn't even print it (how conscientious). He finished the letter, removed the disk from the area and took it home to print the document on his home printer. All went well. Or so it would seem.

Several days later, the employee's son took the disk to school - he had used it to process his homework. The son then loaned the disk to a foreign student who was in need of a disk. Now a foreigner had access to our national security information and to some adverse personal financial information about the trusted employee. It was just that easy! How did it happen? Classified was never written to the disk -- or was it?

Computer Forensics Steps In

The mortgage document was written using a typical word processing program. When the computer creates a document, it does so in clumps



that must be 512 bytes long. This particular mortgage document was only 300 bytes long. After writing the End-of-File, the system needed an additional 212 bytes of information to fill the remaining space . Users do not have the opportunity find information to fill this space -- the computer does it. The additional information needed can be drawn from the unclassified information previously stored on the disk or downloaded from the memory of the classified system that was used to process the Document. If the second scenario is used, there is a good chance that classified information will be written to the disk - without your knowledge and without you being able to check it or remove it. A computer forensics tool would have to be used to

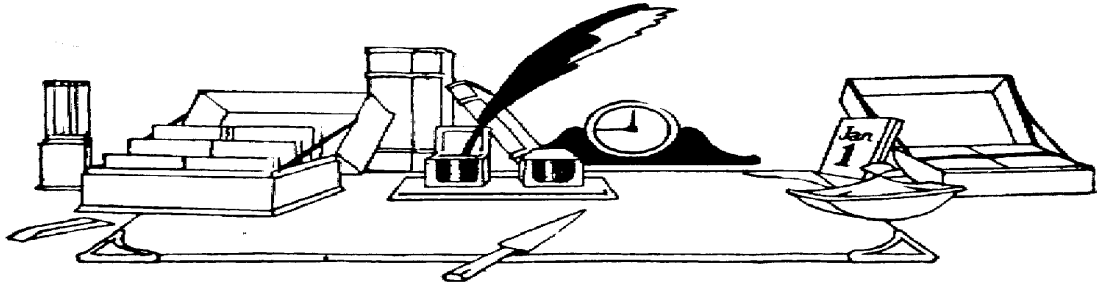
What Went Wrong

The employee:

- brought a disk in from home for use in the program area
- did not check the disk with the ISSO,
- used to disk to process non work related materials on a classified system, and
- removed the disk from a program area without authorization (or checking for contamination.)

An “honest” employee made a very costly mistake. One in which the security of the national defense did not stand a chance. Is this a proven case of espionage? No. Was information compromised to a foreign entity? Definitely

Adhering to AIS security procedures governing the use of magnetic media and AISs inside program areas will prevent these costly mistakes.



Editor's Corner

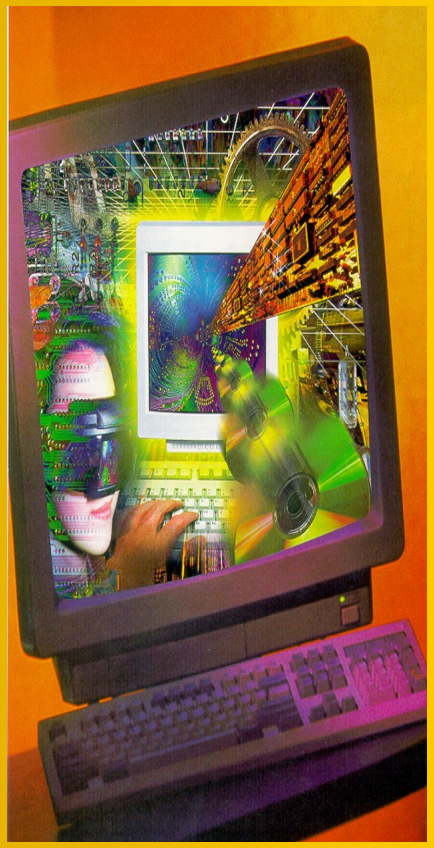
The AIS security awareness quarter provides an opportunity to focus education efforts on the dynamics of AIS/technical security. As seen in the lead article, there's no more room for the inexperienced, unaware novice who "unintentionally" makes a mistake. You are each encouraged to get on board with a heightened awareness of the atrocities associated with poor security practices and the severity of damage one incident can cause to the national security.

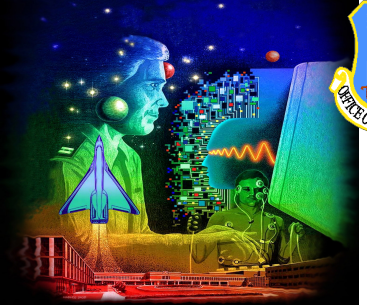
You are each in a position of trust and "responsibility." Careless actions and breaking the rules will not be tolerated if information is to be protected.

I will not allow ignorance to be the downfall of the most powerful nation on earth.,

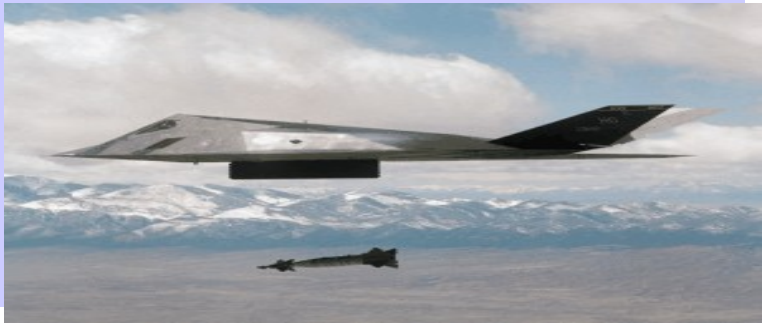
Timothy A. Davis, Security Manager

- Read the AISSP
- Virus Check Software
- Contact Your ISSO
- Brief Visitors on AIS Security Requirements
- Report Anomalies to the ISSO





Counterintelligence Support to Research and Technology Protection



The Air Force's Research and Technology Protection (RTP) Program was developed to identify and protect USAF technical edge data at all levels of the conflict spectrum, prevent compromise or loss of critical program information (CPI), protect USAF critical research and development efforts, and to help the United States maintain its economic competitiveness. Professionals who work in the scientific and technical arena will work hand-in-hand with counterintelligence (CI) professionals as they design and employ effective cradle-to-grave protection methods.

RTP program awareness materials will be disseminated by SASEC members as part of your quarterly security awareness training. Please review the contents of these special reports to ensure you are doing everything you can to protect our valuable information. Get involved in the CPI identification process and RTP program!

Telephone numbers and points of contact are provided in the reports for anyone who may need to contact a CI

Community Oversight Crossfeed

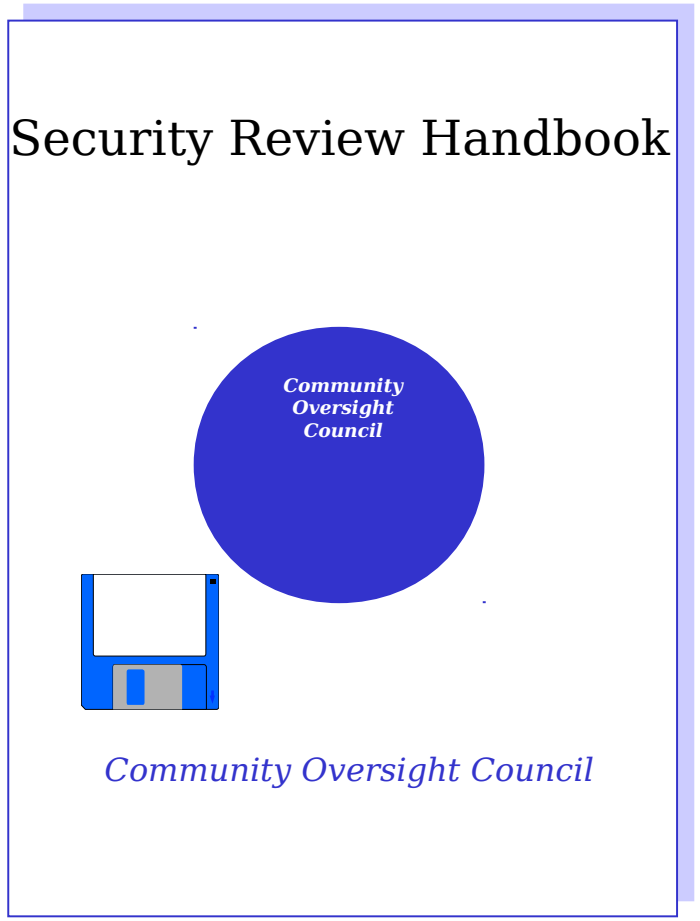
New Community Oversight Council Formed

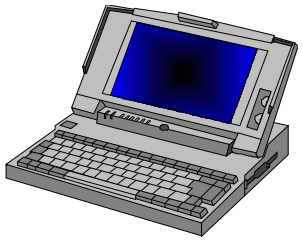
Earlier this year, representatives from throughout the community met to establish the first community-wide Security Review Oversight Council. The mission of the council is to establish the AF SP security review and oversight policy as well a communicate that policy to all concerned parties within the community.

The council will also work together with other services to develop a schedule for security reviews that will meet the requirements and uphold the concept of reciprocity.

The council is currently working on updating AFI 16- 705 and has developed a Security Review Handbook soon to be made available to anyone who will be responsible for conducting security reviews.Training courses will also be developed and offered beginning later in 2001 for team leaders.

The Security Review Crossfeed column will be used to communicate adverse trends and security incidents as



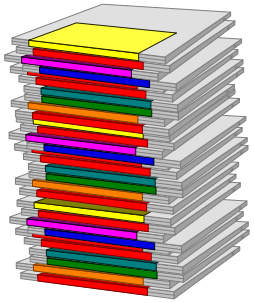


Personal Electronic Devices

Policy for the control and operation of personally owned and small electronic portable devices is currently in the rewrite stage. It is promised to closely resemble the policy already in place by the DIA.

Media Control

Control of magnetic media has long been a concern. As a reminder, all media must enter and exit a program area via the authority of the ISSO. ISSOs ensure all media is virus checked and authorize its use on a system. Users may not bring media into the facility without the permission of the ISSO, must check it immediately with the ISSO upon entering the area, and must ensure that only authorized software and media is used.



This is a great time to review the AIS procedures and plans at your home location and at those locations you frequent throughout the year. Remember to contact the ISSO if you have questions.

NISPOMSUP Chapter 8 Rewrite Status

The May 2000 release is the version currently in use. A follow on product is in coordination and should be released in the near future. The upcoming release will mirror DCID 6-3, Protecting Sensitive Commented Information Within Information Systems.

AIS Vulnerabilities Reporting Security Incidents and Violations

Computers are used for criminal and fraudulent activity more than ever before.Procedures are in place for reporting unauthorized activities or suspicious incidents. Contact your ISSO or PSO if you have a report to make.

SASEC Corner

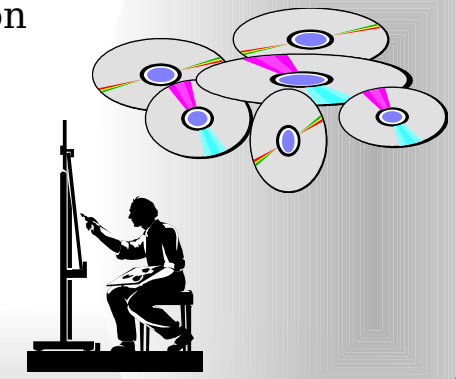
Initial Education

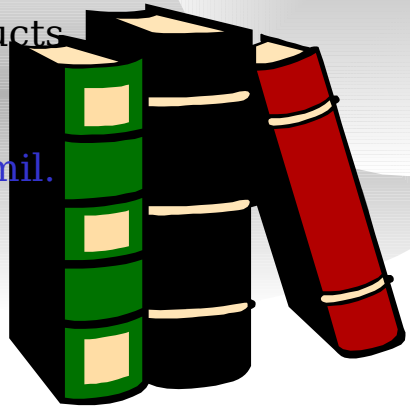
- Program Overview
- "Value" of the Program
- Threat
- Individual Security Responsibilities
- Administrative Security
- AIS Security
- OPSEC

2001 Quarterly Security Awareness

Jan - Mar: Security Management
Apr - Jun: AIS Security
Jul - Sep: Personnel Security
Oct - Dec: Information Security

Available education aids include CDs, reports, booklets and other publications that address password security, internet security, media control, etc. Information assurance products can be ordered from: http://iase.disa.mil.





Your Initial Briefing

Do you remember your initial briefing? A lot of valuable information was presented in a very short time period. You were expected to remember what you were protecting and how to protect it.

For some of you, it may be time again to review the information presented. The chart about outlines what you were told. This is important information that should be remembered.

Education at the National Level

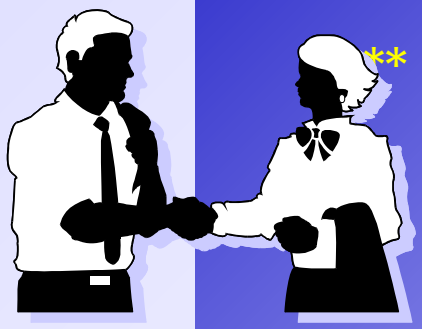
As most of you are aware, the SASEC became involved with national level/ joint security education during the later part of 2000. Our association with the Security Policy Board (SPB) however, came to an abrupt end earlier this year when the SPB was dissolved by a Presidential Directive.

Our SASEC will continue to meet quarterly and invite those contacts in the Army, Navy and various DoD agencies that were developed as a result of our SPB involvement. Continuing our joint relationships will ensure

Technology and the Insider Threat

Years ago, classified paper documents were secured in drawers, inside safes, inside locked rooms. These rooms were in locked buildings, had guards, at installations with perimeter fences and police/guard patrols. In short, they were not easily accessible.

Today, individuals with access to a network can have access to thousands of file cabinets, around the world with impunity and anonymity built in.



In the Next Issue:

**** Highlight on Personnel Security ****

SASEC Corner

Editor's Corner

AIS Security

Policy Corner